Maryland PCI DSS Compliance Policy

Last Updated: 01/31/2017

Contents

1.0 Purpose

The Maryland Department of Information Technology (DoIT) is committed to managing the confidentiality, integrity, and availability of **payment card account data** that is stored, processed, and transmitted electronically via State government Information Technology (IT) networks, systems, and applications (IT Systems).

All card processing activities and related technologies must comply with the **Payment Card Industry Data Security Standard (PCI DSS)** in its entirety. Card processing activities must be conducted as described herein and in accordance with the standards and procedures listed in section 4.0 of this policy. No activity may be conducted nor any technology employed that might prevent compliance with any portion of the PCI-DSS. The Maryland Department of Information Technology (DoIT) will utilize requirements as outlined by the PCI DSS version 3.2 (April 2016) to establish this policy and protect cardholders against misuse of their personal information and to minimize payment card losses.

2.0 Document and Review History

This document will be reviewed annually and is subject to revision.

Date	Version	Policy Updates	Approved By:
01/31/2017	v1.0	Initial Publication	Maryland CISO

3.0 Applicability and Audience

This policy is applicable to all system components included in or connected to cardholder data environments that store, process, or transmit cardholder data or sensitive authentication data. System components include, but are not limited to the following: network components, servers, or applications included in or connected to the cardholder data environment. Information Technology (IT) assets utilized by any agency supported by, or under the policy authority of, the Maryland Department of Information Technology and considered a **merchant** within the definition of PCI DSS must comply with the requirements of this policy. Any vendor used by a State of Maryland Executive Branch agency to store, process, or transmit cardholder data must be PCI DSS compliant and must update the agency as to PCI DSS compliance status on a yearly basis.

NOTE: This policy provides guidance for compliance with the main requirements of the PCI DSS but does not supplement, replace, or supersede the PCI DSS itself. Agencies should exercise due care to comply with the requirements as outlined by the PCI DSS.

4.0 Policy

This policy describes an overall strategy to comply with the six core principles and twelve top level requirements of PCI DSS.

Agencies shall eliminate the collection and storage of unnecessary data, restrict cardholder data storage to as few locations as possible, and isolate the cardholder data environment from the rest

of the network, where possible. Compliance with PCI DSS is an on-going process and defined as a business-as-usual approach, meaning that controls and compliance with PCI DSS must be included in the overall risk-based security strategy of the organization.

4.1 Account Data

Account data consists of cardholder data and sensitive authentication data as outlined below.

Cardholder Data	Sensitive Authentication Data
Primary Account Number (PAN)	Full magnetic stripe data or equivalent data on a chip
Cardholder name	CAV2/CVC2/CVV2/CID
Expiration date	PINs/PIB blocks
Service code	

PCI DSS requirements apply to merchants who store, process, or transmit Primary Account Numbers (PAN), and in accordance with PCI DSS, PANs and other type of cardholder data must be stored in an unreadable format (e.g., encrypted, truncated, etc.). Sensitive authentication data may never be stored post-authorization, even if encrypted.

4.2 Summary of Requirements

Core Principles	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data
	2. Always change vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update antivirus software or programs
	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know
	8. Identify and authenticate access to system components
	9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

4.3 PCI Compliance Validation

The Payment Card Industry uses merchant levels to determine risk and designate the appropriate level of security for the business. Merchant levels determine the assessment rigor and security validation required for a merchant to pass PCI DSS assessment. Each payment card brand has the option of modifying merchant levels.

Visa and MasterCard brand levels and requirements are outlined below as an example; the PCI DSS itself has details of other payment card brand requirements.

Visa and MasterCard Requirements	
Merchant Levels	**Assessment Requirements**
Level 1 ▪ Merchant that processes over six million Visa payment card transactions annually (all channels); ▪ Merchant that has had a data breach or attack that resulted in an account data compromise; or ▪ Merchant that has been identified by any card association as Level 1.	▪ Annual **Report on Compliance** ("**ROC**") by **Qualified Security Assessor** ("**QSA**") – also commonly known as a Level 1 onsite assessment - or internal auditor if signed by officer of the company; ▪ Quarterly network scan by **Approved Scan Vendor** ("**ASV**"); ▪ **Attestation of Compliance Form**.
Level 2 Merchant that processes one to six million Visa transactions annually (all channels).	▪ Annual **Self-Assessment Questionnaire** ("**SAQ**"); ▪ Quarterly network scan by ASV; ▪ Attestation of Compliance Form.
Level 3 Merchant processing 20,000 to one million Visa e-commerce transactions annually.	▪ Annual SAQ; ▪ Quarterly network scan by ASV; ▪ Attestation of Compliance Form.
Level 4 Merchants processing fewer than 20,000 Visa e-commerce transactions annually, and all other merchants processing up to one million Visa or MasterCard transactions annually.	▪ Annual SAQ; ▪ Quarterly network scan by ASV; ▪ Attestation of Compliance Form.

NOTE: Each payment card brand has its own requirements and merchants must exercise due diligence and due care to comply with the specific requirements of the payment card brands they process.

4.4 Breach Notification

Agencies must notify consumers of any breach of PCI information in accordance with the notification requirements set forth by the payment card brands they process. Additionally, PCI DSS supplements, but does not superseded State laws and regulations outlining requirements associated with what constitutes a breach, requirements for notice, and exemptions. Merchants covered by PCI DSS must ensure compliance with all Maryland security breach laws, such as Md. State Govt. Code §§ 10-1301 to 1308.

4.5 PCI DSS Penalties for Noncompliance

Agencies considered merchants under PCI DSS must take due care and due diligence to abide by the respective standards set forth by the payment card brands that they process. Noncompliance penalties can vary at the payment card brand's discretion. Fines to acquiring banks can range per month and per incident for PCI compliance violations. Banks require indemnification of this fine and pass this fine on to the merchants.

Merchants who do not comply with PCI DSS may also face other consequences, including but not limited to: responsibility to reimburse fraud losses, increased transaction fees, and incurring the cost of reissuing cards and providing monitoring services to affected consumers.

5.0 Exemptions

The requirements of this policy are established by the Payment Card Industry Security Standards Council, there are no exemptions to this policy.

6.0 Policy Mandate and References

The Payment Card Industry Security Standards Council and the DoIT Cybersecurity Program Policy mandate this policy. Related policies include:

- Account Management Policy
- Boundary Protection and Internet Access Policy
- Cybersecurity Authority to Operate Policy
- Security Assessment Policy

7.0 Definitions

Term	Definition
Annual Self-Assessment Questionnaire (SAQ);	Self-assessment questionnaire that can be completed by merchants themselves as proof of compliance with the PCI DSS. There are different categories of SAQs, which depend on the payment card channels used by the vendor.
Approved Scan Vendor (ASV)	An organization offering security services and tools (e.g., ASV scan solution) to conduct external vulnerability scanning services.
Attestation of Compliance Form	Document completed by a Qualified Security Assessor (QSA) or merchant (if merchant internal audit performs validation) as a declaration of the merchant's compliance with the PCI DSS.
Merchant	Defined as any entity that accepts American Express, Discover, JCB, MasterCard, or Visa payment cards as payment for goods and/or services (including donations).
Payment Card Account Data (Account Data)	Consists of cardholder data and/or sensitive authentication data.
Payment Card Industry Data Security Standard (PCI DSS)	A proprietary information security standard for organizations that handle credit cards from the major card companies, including American Express, Discover, JCB, MasterCard, or Visa.

Term	Definition
Qualified Security Assessor (QSA)	An organization that has been qualified by the PCI Council to have their employees assess compliance with the PCI DSS.
Report on Compliance (ROC)	Report on assessment that tests procedures specific to each PCI DSS requirement and conducted by a Qualified Security Assessor (QSA) or an Internal Security Assessor (ISA).

8.0 Enforcement

In addition to any fines and/or penalties imposed by payment card brands, if DoIT determines that an agency is not compliant with this policy, the agency will be given a sixty (60) day notice to become compliant or at least provide DoIT a detailed plan to meet compliance within a reasonable time before issue is reported to the Secretary of Information Technology. The Secretary of Information Technology, or a designated authority, may extend a non-compliant agency's window of resolution or authorize DoIT to shutdown external and internal network connectivity until such time the agency becomes compliant. Any vendor used by a State of Maryland Executive Branch agency found to be non-compliant with PCI DSS will be considered to be in violation of this policy.

Any personnel attempting to circumvent PCI DSS, such as stealing payment card data, improperly accessing, or intentionally manipulating payment card data will be investigated as a security violation and subject to disciplinary action, which may include written notice, suspension, termination, and possible criminal and/or civil penalties.